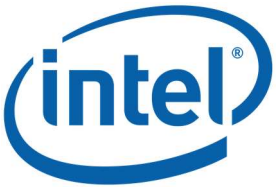

Intel® Bluetooth® Security – Encryption Key Size Recommendation

White Paper

August 2019

Revision 1.0

Contents

Revision History

Revision	Description	Date
1.0	Initial release	August 2019

References

[ref 1] Guide to Bluetooth Security, NIST Special Publication 800-121 Revision 2.
https://doi.org/10.6028/NIST.SP.800-121r2

[ref 2] CVE-2019-9506
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9506

[ref 3] Bluetooth® Expedited Errata Correction 11838: Encryption Key Size Updates.
https://www.bluetooth.com/security/statement-key-negotiation-of-bluetooth

1 Introduction

Bluetooth® technology has been part of the Intel® Wireless products for many years and is now prevalent in laptops and desktops. Some of the main usages of Bluetooth on the PC are; providing access to a wireless keyboard and mouse, streaming audio to headphones or speakers, performing data transfers or providing location services.

Billions of Bluetooth devices are shipped annually, and shipments are projected to grow steadily over the coming years.

The number of threats to the Bluetooth wireless technology also continues to grow, with new attack vectors over the wireless network such as denial of service (DoS), eavesdropping, man-in-the-middle (MITM) attacks etc.

The Bluetooth communication between two connected devices typically involves the following components on both sides of the link: a hardware Bluetooth Controller and a software Bluetooth Host with Bluetooth Profiles/Services that are typically part of the Operating System.

To improve the security of Bluetooth implementations, **Intel highly recommends** that the guidelines/security recommendations described in the *'Guide to Bluetooth Security, NIST Special Publication 800-121 Revision 2'* [ref 1] are followed.

In response to the *'CVE-2019-9506'* vulnerability [ref 2] describing a MITM attack during the encryption key size negotiation procedure and the published *'Bluetooth Expedited Errata Correction 11838: Encryption Key Size Updates'* from the Bluetooth SIG [ref 3], Intel provides the recommendations below.

2 Encryption Key Size Recommendations

According to the NIST paper [ref 1, section 3.1.3]

"The encryption key (KC) may vary in length in single byte increments from 1 byte to 16 bytes in length, as set during a negotiation process that occurs between the master and slave devices. During this negotiation, a master device makes a key size suggestion for the slave. The initial key size suggested by the master is programmed into the controller by the manufacturer and is not always 16 bytes. In product implementations, a "minimum acceptable" key size parameter can be set to prevent a malicious user from driving the key size down to the minimum of 1 byte, which would make the link less secure."

NIST also states [ref 1, section 4.4, item #23]

Item	*Security Recommendation*	*Security Need, Requirement, or Justification*
23	*Configure encryption key sizes to the maximum allowable.*	*Using maximum allowable key sizes provides protection from brute force attacks.*

Intel Bluetooth Controller implementations support encryption key sizes from 1 byte to 16 bytes in length supported by the Bluetooth specification. Intel Bluetooth Controllers always use the maximum allowed key size supported by the specification as the initial key size for the negotiation process.

Intel highly recommends that Bluetooth Controllers use the highest allowable value for the encryption key size.

From the Bluetooth SIG Errata [ref 3, Volume 3, Part C: Generic Access Profile]

"A device shall enforce an encryption key with at least 128-bit equivalent strength for all services that require Security Mode 4, Level 4. For all other services that require encryption, a device should [emphasis added] enforce an encryption key with at least 56-bit equivalent strength, irrespective of whether the remote device supports Secure Simple Pairing.

After encryption has been enabled, the Host should check the encryption key size using either the HCI_Read_Encryption_Key_Size command (see [Vol 2] Part E, Section 7.5.7) or a vendor-specific method."

Intel highly recommends that the Bluetooth Host use the highest allowable value for encryption key sizes for all services that employ encryption.

Intel Bluetooth Controller implementations support the HCI_Read_Encryption_Key_Size command to allow the Bluetooth Host to enforce minimum encryption key sizes.

3 Summary

Intel highly recommends that all components participating in a secure Bluetooth connection (Bluetooth Controller, Bluetooth Host and Profiles/Services) employ the highest level of encryption.